ABSTRACT

Provided is a content distribution system that prevents different keys to be derived between an encryption apparatus and a decryption apparatus. A random-number generating unit 112d, in an encryption apparatus 110d, generates a random number s, and a first function unit 113d generates a functional value G(s) of the random number s, and generates a verification value a and a shared key K from the functional value G(s). An encryption unit 114d generates a first cipher text c1 of the verification value a using a public-key polynomial h, and a second function unit 115d generates a functional value H(a,c1) of the verification value a and the first cipher text c1, and a random-number mask unit 116d generates a second cipher text c2=s xor H(a,c1). A decryption unit 123d, in a decryption apparatus 120d, decrypts the first cipher text c1 using a secret-key polynomial f, to generate a decryption verification value a'. A third function unit 124d generates a functional value H(a',c1) of the decryption verification value a' and the first cipher text c1, and a random-number mask removal unit 125d generates a decryption random number s'=c2 xor H(a',c1). A fourth function unit 126d generates a hash functional value G(s') of the decryption random number s', and generates a verification value a'' and a shared

key K′ from the functional value G(s′). A comparison unit 127d outputs the shared key K′ if the decryption verification value a′ is equal to the verification value a′′.